REMARKS

In the December 15, 2004 Office Action, the Examiner noted that claims 1-20 were pending in the application; objected to the Abstract; rejected claims 1-20 under the second paragraph of 35 USC § 112; rejected claims 1-3, 6, 8, 11-13, 16 and 18 under 35 USC § 102(b); and rejected claims 5, 7, 9, 10, 17, 19 and 20 under 35 USC § 103(a). In rejecting the claims, U.S. Patent 5,201,000 to Matyas et al. and a book by Menezes et al. (References A and U, respectively) were cited. Claims 4 and 12-20 have been cancelled and claims 21-23 have been added. Thus, claims 1-3, 5-11 and 21-23 remain in the case. The Examiner's rejections are traversed below.

The Application

The application relates the following scenario. A user generates an asymmetric cryptographic key pair having a private key and a corresponding public key. To this end, the user generates two prime numbers and, then, derives the private key as well as the public key from these two prime numbers. Then, the user distributes the public key and, importantly, erases the private key. Thus, the user does not have to store the private key, which is of course a very sensitive information for the user on the computer or a chip card etc. Thus, nobody can retrieve the user's private key from a chip card or a computer or a laptop etc., since the private key is simply not there.

When the user needs the private key for digitally signing a document or for decrypting a message of a communication partner, which is encrypted using the public key (which the user distributed to the communication partner earlier), then the user has to re-generate a private key. This "re-generated" private key is also referred to as a "secret communication key" in the application. Naturally, the regenerated secret communication key to be re-generated by the user has to be identical to the private key of the asymmetric cryptographic key pair, which the user generated earlier and which the user has erased as out-lined above.

Thus, the user now has the task to determine exactly the same private key, i.e., the regenerated private key, which the user determined and erased earlier.

Objection to Abstract

Submitted herewith is a Substitute Abstract in response to the objection in the Office Action. Withdrawal of the objection is respectfully requested.

Rejection under 35 USC § 112, Second Paragraph

In items 5-13 on pages 2-4 of the Office Action, claims 1-20 were rejected under the second paragraph of 35 USC § 112 for indefiniteness. Claims 4 and 12-20 have been cancelled and claims 1-3 and 5-11 have been amended. In the remaining claims, it is believed to be substantially self-explanatory with regard to how the Examiner's objections have been addressed. However, with regard to the Examiner's objection in item 12 of the Office Action, the terms "Miller-Raven" and "RSA" are well known methods at least described in the Handbook of Applied Cryptography (reference AT cited by Applicant). For example, the Miller-Raven primarity test is described in Section 4.2.3 of the Handboodk, which starts on page 138 and ends on page 140. The RSA method is described in Section 8.2 of the Handbook of Applied Cryptography, which appears on pages 285-289 of the handbook. Because these terms are well-known, it is submitted that their use in the claims is fully appropriate.

Rejection under 35 USC § 102(b)

The claimed way of originally generating the private key and re-generating the private key (the re-generated private key corresponds to the secret communication key) distinguishes the present invention over Matyas et al. As described in the application, the original generation of the predetermined asymmetric cryptographic key pair takes place as follows (please note that corresponding, but not necessarily the same, steps are included in the first paragraph of amended claim 1 and the steps/features of new claims 21 and 23):

The user inputs his password or personal identification number or something else, which the user can remember easily. This password or PIN etc. are examples for the "predetermined initial value" in claim 1. Then, this predetermined initial value is processed, preferably using a hash function (see claim 2). Performing this step of processing with or without the hash function results in the base value BW for obtaining the two prime numbers (p, q). See Fig. 3.

In Fig. 3, the base value BW is checked for primality. If the base value BW is a prime number, then the first prime number p is already present and the index for the first prime number p is equal to zero. When, however, the base value BW is not a prime number, or for determining the second prime number q, when the base value BW is determined to be the first prime number p, the base value BW is increased by a predetermined value (such as the number "+ 2" in Fig. 3) to result in an increased value W1. Then, this value W1 is examined for primality and the index is set to 1. If W1 is a prime number, then an index of "1" is stored.

If W1 is not a prime number, the whole procedure is repeated. Assume the situation when W is not a prime number, but W3 is a prime number. Then, the "initial" generation of the prime number results in the prime number W3 on the one hand and the stored Index A3 on the other hand.

For re-generating the private key, which means for re-generating the prime numbers p, q, it is not necessary to again conduct the same iterative checking for primality, increasing by the predetermined value, again checking for primality, storing an index, etc. Instead, for re-generating the prime numbers, only the base value (obtained from the predetermined initial value), and the stored index are necessary. For re-generating the prime number W3 for example, only the base value has to be generated from the predetermined initial value. Then, the base value only has to be increased by the product of the predetermined increment and the stored index to immediately arrive at the prime number W3 which can be used for the final calculation of the regenerated private key in a straight-forward manner.

To summarize, even if the method is cumbersome when the initial private key/public key determination is performed, the later efficiency is more important. In the initial private key/public key determination, there is an iterative process and potentially a high number of primality tests, which can consume a considerable amount of processing power.

On the other hand, when re-generating the private key or the "secret key," which of course must match the original private key, the process is very efficient, since the base value only has to be increased by a value determined by the stored index and the predetermined increment to automatically arrive at the desired prime number. Thus, when re-generating the prime numbers for calculating the regenerated private key, the process does not perform any iterative process or any primality tests involving a high amount of processing power.

Thus, the process is especially suited for use in small devices, which do not have such large amounts of processing power, such as mobile telephones, palm computers, or, in general, any device based on chip cards, on which the calculations are performed. By reducing the amount of processing by not performing any iterative process or any primality tests when forming the regenerated private key, a substantial amount of battery power is saved, which is especially advantageous in battery-driven mobile phones, or any other hand-held device such as a palm computer.

Support for the claim amendments is as follows.

The amendments to the first paragraph of claim 1 are supported by claim 4, page 6, lines 14 to 25 and page 7 and page 8. These text passages also support new claims 21, 22, and 23.

Please note that these new claims relate to a situation where the asymmetric cryptographic key pair is initially generated.

The amendments in the last four paragraphs of claim 1 and the corresponding amendments in the apparatus claim 11 are supported by page 9, lines 8 to 18.

Referring now specifically to Matyas et al., please refer to Fig. 7, which shows the key generation algorithm. Generally, a trial value of p is generated and tested for primality. Additionally, a trial value of q is generated and tested for primality. This key generation algorithm is invoked several times, after the 1 to 8-bit hash value CW is formed using an input pass phrase PP as outlined in column 19, lines 9 to 11. Additionally, please refer to column 18, lines 13 to 24. A first seed for a dynamically seeded pseudo random number generator 200 in Fig. 14 is calculated from the pass phrase. Then, the output of the dynamically seeded pseudo random number generator is tested by the key generation algorithm for primality. When the output is a prime number, the public key PU and the private key PR are generated and output via line 64 in Fig. 14. When, however, the output provided by line 56 does not pass the primality test, the output of the dynamically seeded pseudo random number generator is again input as a new seed and the output of the pseudo random number generator in response to the new seed is again input into the key generation algorithm to check whether this value is a prime number or not. This procedure is repeated until prime numbers have been detected so that the public key PU and the private key PR can be calculated. Please refer to column 18, lines 25 to 30. It should be clear that in Matyas et al. that there is no way to know in advance how many trials are needed before finding values that are satisfactory, since the process is one of trial and error.

Matyas et al. is silent on storing the number of trials as an index. Additionally, storing the number of trials would not make any sense, since the finally determined numbers do not deterministically depend on the number of trials, Matyas et al. is also silent on increasing a number by a predetermined increment. Instead, Matyas et al. relies on a dynamically seeded pseudo random number generator.

To summarize, the Matyas et al. method for generating the prime numbers, which are the basis for calculating the public key and the private key, may be somewhat analogous to the invention when the private key is initially generated. However, the two methods are very different when the private key is regenerated.

When a regenerated private key is to be produced in the Matyas et al. device, exactly the same procedure has to be performed, i.e., seeding the dynamically seeded pseudo random number generator, testing the output for primality using the key generation algorithm and again seeding the pseudo random number generator using the output from the last trial to obtain a new trial value, etc. With the claimed invention, regeneration of the private key is much simpler than initially generating the private key.

The Matyas et al. procedure is disadvantageous in that a dynamically seeded pseudo random number generator has to be used for the initial private key generation and, in addition, has to be used to produce the regenerated private key.

This prior art procedure requires the same trial and error procedure using the sophisticated dynamically seeded pseudo random number generator, which results, in particular for a hand-held battery-powered device, in a high processing load and a high power consumption.

Summary

It is submitted that the references cited by the Examiner, taken individually or in combination, do not teach or suggest the features of the present claimed invention. Thus, it is submitted that claims 1-3, 5-11 and 21-23 are in a condition suitable for allowance. Reconsideration of the claims and an early Notice of Allowance are earnestly solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: April 15 2003

By: Mark J. Henry
Mark J. Henry
Registration No. 36,162

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

CERTIFICATE UNDER 37 CFR 1.8(a)
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on April 15, 2003
STAAS & HALSEY
By: Mark J. Henry
Date: 4.15.03